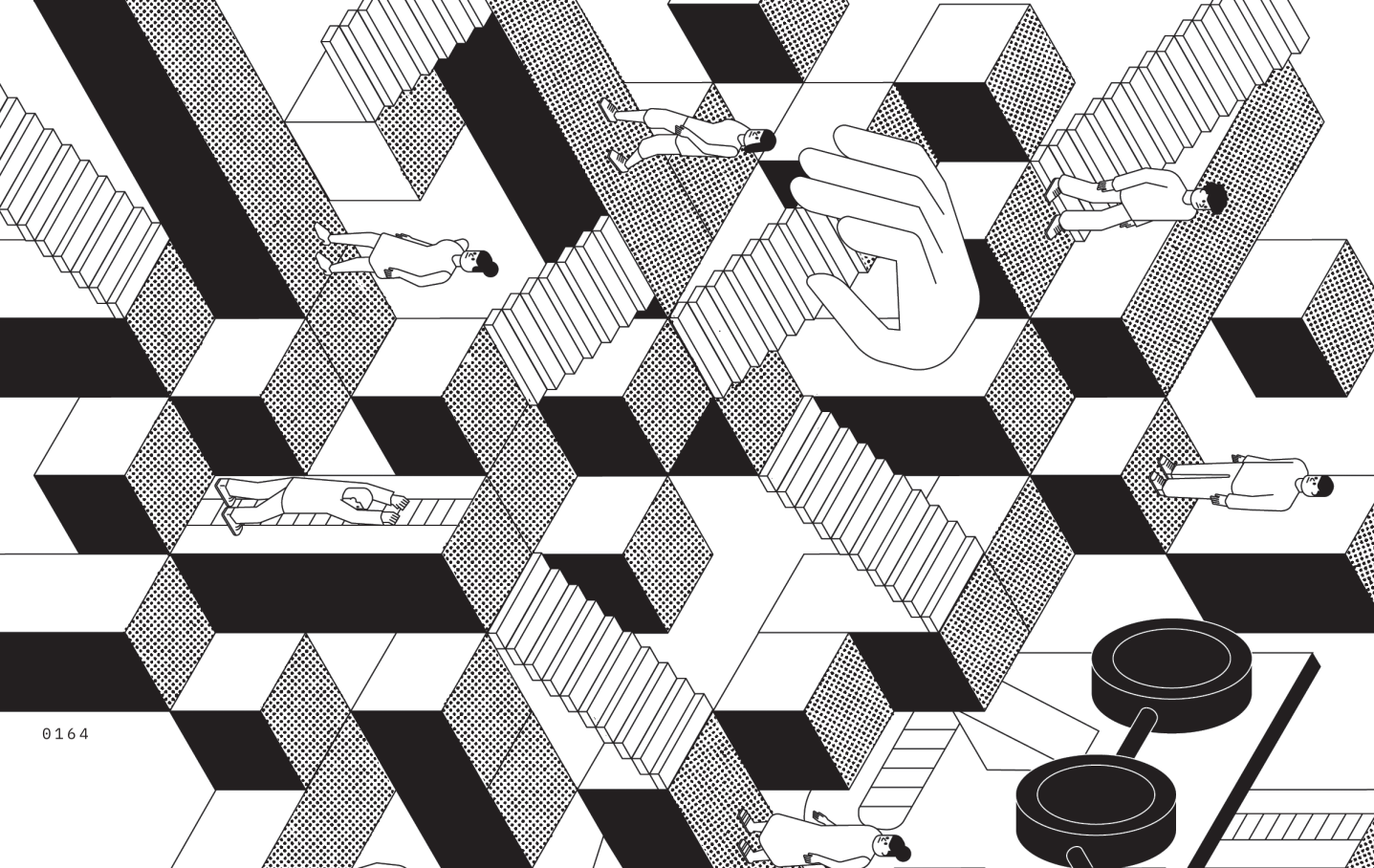
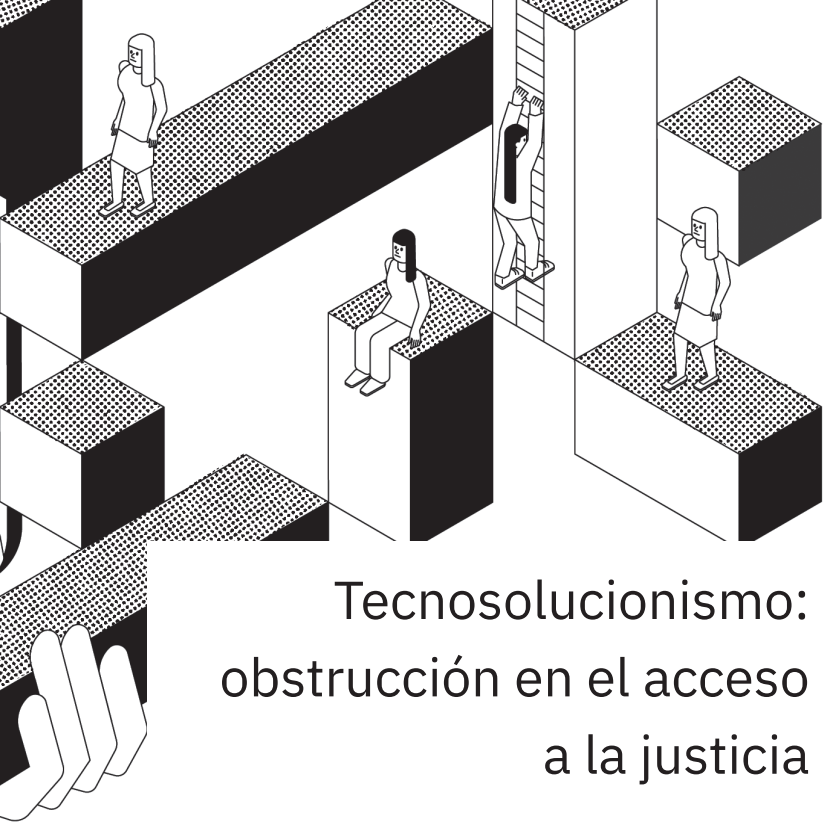


0164



Tecnosolucionismo: obstrucción en el acceso a la justicia

ALEX ARGÜELLES

Alex Argüelles es tecnólogue, licenciade en comunicación y fundadore del Laboratorio de resiliencia digital **comun.al**. Desde 2013 colabora en iniciativas sobre derechos humanos y tecnologías en América Latina; realizando procesos de incidencia y análisis con énfasis en privacidad, género, accesibilidad e inclusión. Facilita talleres y provee acompañamiento en seguridad digital a periodistas, comunicadoras y activistas en la región desde un enfoque psicosocial, con aproximaciones para la justicia transformativa. Actualmente forma parte del programa de Tecnología y Sociedad de la Fundación Mozilla, abordando la violencia sociopolítica ejercida a través de las tecnologías en México.

CUANDO ENFRENTAMOS VIOLENCIA digital, lo primero que suele venir a la mente es qué hay que hacer para restablecer la seguridad de nuestros dispositivos o cuentas. Queremos recuperar el control de nuestra información e incluso identificar el origen del ataque o la violencia que estamos recibiendo. Una vez que tenemos algunas ideas sobre cómo accionar a partir de esto, buscamos mecanismos de reporte o denuncia, buscamos el acceso a la justicia frente las agresiones que vivimos, pero ¿qué significa justicia y cómo podemos acceder a ella?, ¿en qué términos —o los términos de quién— se define el acceso a la justicia?

La justicia tiene varios significados. Podemos pensarla como un bien común, como una condición indispensable para el desarrollo de las personas, como el conjunto de criterios que establecen los límites en las relaciones donde participamos (como individuos, como integrantes de la sociedad, como sujetos políticos, etcétera), a fin de que en estas relaciones diversas se respeten los derechos humanos y se establezcan condiciones que nos permitan ejercerlos de la manera más amplia posible. De acuerdo con las apuestas políticas de la justicia transformativa, podemos pensar la justicia como una respuesta a la violencia, al daño y al abuso que busca la restauración, la sanación y la transformación tanto de las personas involucradas como de sus entornos para prevenir la propagación de las violencias procurando la corresponsabilidad y la

resiliencia comunitarias. En teoría, el Estado —también en México— tiene entre sus funciones procurar la justicia por la autoridad que posee sobre su territorio y quienes lo habitan.

Volviendo al ejemplo de violencia digital, es interesante ver cómo en los últimos diez años se ha ido desarrollando un discurso incongruente en torno a las formas en las que el Estado provee respuestas o "justicia" a las situaciones en las que existen violencias propagadas a través de tecnologías, mientras refuerza el uso de tecnologías como una forma de consolidar las capacidades de control para mejorar la "seguridad" que nos ofrece. Entrecomillo justicia y seguridad porque estos conceptos han sido tan reducidos, desde la argumentación de los sesgos de quienes nos gobiernan, que terminan convirtiéndose en evidencia de la falta de habilidades para entender y atender la complejidad que los caracteriza.

En respuesta a la violencia digital, particularmente la violencia de género, se han creado dependencias especializadas en "ciberdelitos" e incluso se han incorporado reformas a leyes para amplificar los tipos penales que existen, a fin de que se contemplen algunas manifestaciones de las violencias que ocurren a través de las tecnologías. Como en muchos otros frentes en los que se defiende la dignidad en la búsqueda de justicia, la lucha por el reconocimiento de los efectos de las violencias digitales fue llevada por personas que anteriormente habían sido victimizadas por esas violencias y quienes fueron revictimiza-

das por el Estado, negándoles el acceso a la justicia: escudándose en la negligente carencia de perspectiva de género y la falta de herramientas necesarias para ser consecuentes con sus responsabilidades que —así como las violencias— también se trasladan a los entornos digitales. La toma de conciencia y el desarrollo de medidas para responder a la violencia de género que se manifiesta a través de las tecnologías en México es un logro de las personas que se organizaron para desarrollar y compartir habilidades con otras que estaban atravesando situaciones similares, como ha sido el caso de la activista Ana Baquedano; pero también es un logro de las personas que convocaron a otras por sus habilidades legales y comunitarias para incidir en el desarrollo de reformas legales promoviendo el reconocimiento de la gravedad de estas violencias, como fue el caso del Frente Nacional para la Sororidad y las Defensoras Digitales en sus diversos capítulos a lo largo del país.

Por otro lado, está la mirada más "industrial" de todo esto. En este campo no se habla tanto de violencia digital, sino más bien de "cibercrimen" o "ciberdelito". Y a lo que se refieren como cibercrimen puede ir desde la suplantación de identidad para realizar fraudes bancarios, hasta las presuntas violaciones a derechos de autor que, como hemos visto en varios casos, más allá de proteger los intereses de las personas creadoras o las industrias de propiedad intelectual, han sido usadas como un mecanismo ágil para la

censura y remoción de contenidos por parte del Estado. Aquí es donde los intereses del Estado y las diversas industrias que han incorporado las tecnologías digitales en sus entornos muchas veces coinciden, pero también entran en desacuerdo con el interés público y muchas veces terminan obstruyendo el ejercicio de los derechos humanos.

En ambos casos, cuando hablamos de violencia digital y cuando se habla de "cibercrimen", vemos cómo se han desarrollado respuestas para atender los daños que se contemplan en las normativas vigentes, sin embargo, cuando observamos el tratamiento que se da a los intereses de la sociedad civil frente a los intereses de las industrias o el Estado la diferencia es clara. El reconocimiento de la violencia digital y sus efectos ha sido parte de una lucha constante de la sociedad civil organizada (liderada por mujeres cis y trans e integrantes de la comunidad LGBTIQ+), que en ese reconocimiento de la gravedad que tiene la violencia digital —como continuación de la violencia machista, misógina, sexista que vivimos diariamente en los entornos físicos— ha exigido el acceso a la justicia que por muchos años fue negada. Sus matices, además, también se extienden a cuestiones en las que la libertad de expresión y la violencia contra periodistas, activistas y personas defensoras de derechos humanos en el país se intersecan con las brechas de desigualdad y el acceso a la información, la educación, la salud o la cultura; mientras

que el “cibercrimen” o los “ciberdelitos” han servido para retomar conversaciones en torno a medidas de persecución, intervención de dispositivos y vigilancia masiva, que consolidan las capacidades de control por parte del Estado bajo el pretexto de que en el uso de tecnologías cada vez más abusivas está la clave para protegernos de potenciales cibercriminales o ciberdelincuentes. Sobre este discurso, se ha señalado anteriormente que un Estado que presume que todas las personas que gobierna son potenciales delincuentes es un Estado que busca instaurar la criminalización como forma de gobierno, omitiendo la presunción de inocencia, apostando a la vigilancia y al castigo para controlar a quienes viven como sospechosas perpetuas, sin respuestas que transformen las situaciones de desigualdad, aborden los diversos contextos en su complejidad ni brinden acceso a la justicia.

El prefijo ciber, en el último caso, permite una nueva categoría de eufemismos que el Estado y sus representantes —en las distintas ramas del gobierno— han sabido instrumentalizar para vigilar, castigar, perseguir y criminalizar con herramientas tan potentes como sofisticadas... Monopolizando la “violencia legítima”, también a través de las tecnologías. Estos eufemismos reclaman un poder especial cuando vemos cómo han sido utilizados en los discursos que han promovido estrategias de seguridad por parte del Estado que vienen acompañadas de la implementación de tecnologías que afectan directa-

mente derechos fundamentales, como el derecho a la privacidad o hasta la libertad de expresión y el acceso a la información.

Los despliegues de estas tecnologías, su instrumentalización con fines abusivos para la consolidación del poder y el desarrollo de legislaciones que se inclinan hacia el desarrollo de políticas públicas que centran su eficiencia en el uso de tecnologías son algunos ejemplos de cómo se manifiesta el tecnosolucionismo: una forma hipersesgada de abordar los problemas complejos, a fin de demostrar una correlación simplificada entre la implementación de algunas tecnologías y los efectos deseados para manejar situaciones que hasta ahora no han logrado ser resueltas por parte del Estado.

Podemos encontrar un ejemplo claro de esta ambivalente aproximación a la justicia en relación con las tecnologías en la consolidación del acceso a internet como derecho constitucional en México durante el 2013. El reconocimiento de este derecho tiene que ver con las posibilidades que brinda internet para amplificar el ejercicio de otros derechos, como son: el acceso a la información y la libertad de expresión, que, a su vez, son fundamentales para el desarrollo individual y social necesarios para que la democracia pueda manifestarse y ejercerse de forma plena.

Sin embargo, la misma reforma que llevó a que se estableciera este derecho en nuestro país venía con una serie de leyes secundarias en las que se establecían posibilidades que por un lado be-

neficiaban a los monopolios de telecomunicaciones, a través de la autorización del menoscabo de la neutralidad de la red —un principio fundamental para el acceso libre a la información sin discriminación por su origen, plataforma o formato en el flujo de internet— para beneficiar los intereses del mercado; mientras que por el otro, ofrecían vías para legitimar abusos de poder a través de las tecnologías por parte del Estado, como el bloqueo de servicios de telecomunicaciones o el seguimiento de la actividades digitales a través de tecnologías de geolocalización: en tiempo real y sin necesidad de aprobación judicial previa.

En abril de 2014 varias personas salimos a tomar las calles para manifestarnos en contra de estas leyes secundarias, exigiendo que se respetara la neutralidad de la red y nuestro derecho a la privacidad como garantías para el ejercicio de la libertad de expresión y el derecho de acceso a la información. En julio de ese año, se promulgó una nueva reforma a la Ley Federal de Telecomunicaciones y Radiodifusión que en su Artículo 145 establece que el Instituto Federal de Telecomunicaciones (un órgano constitucional autónomo creado un año antes para regular y supervisar tanto las redes como los servicios de telecomunicaciones y radiodifusión en el país) debía expedir una serie de lineamientos para asegurar la neutralidad de la red conforme a los principios de: libre elección, no discriminación, privacidad, transparencia e información, gestión

de tráfico, calidad y desarrollo sostenido de infraestructura. El Artículo 146 de esta ley también determina que: "Los concesionarios y los autorizados deberán prestar el servicio de acceso a internet respetando la capacidad, velocidad y calidad contratada por el usuario, con independencia del contenido, origen, destino, terminal o aplicación, así como de los servicios que se provean a través de internet, en cumplimiento con lo señalado en el artículo anterior".

Para enero de 2019, el IFT seguía sin expedir los lineamientos que permitirían salvaguardar la neutralidad de la red y los derechos que han sido afectados por la falta de mecanismos para resguardar la privacidad, el acceso a la información y la libertad de expresión. Frente a esto la Red en Defensa de los Derechos Digitales presentó un amparo para exigir al IFT el cumplimiento de su obligación de expedir estos lineamientos. Esta demanda de amparo favoreció a la sociedad civil y obligó al IFT a presentar los lineamientos pendientes a más tardar durante el segundo trimestre del año 2021. En diciembre de 2019 el IFT puso a consulta pública el anteproyecto de lineamientos para la gestión de tráfico y administración de la red, que según lo establecido por el mismo IFT tiene por objetivos:

i) Garantizar que el usuario final tenga libertad de decisión sobre los contenidos, aplicaciones y servicios a los que accederá, así como conocimiento de la

forma en que se gestiona su tráfico en la red.

ii) Otorgar certidumbre jurídica a la industria en materia de neutralidad de red, dando claridad sobre las políticas de gestión de tráfico y administración de red viables, así como respecto de las prácticas comerciales admisibles.

iii) Fomentar la innovación del sector mediante el uso de tecnologías más eficientes en el uso de las redes y en nuevas estrategias comerciales.

iv) Favorecer la disminución de la brecha digital, a través de ofertas comerciales alineadas con las políticas de gestión de tráfico y administración de red autorizadas por el instituto, con objetivos específicos.

v) Promover condiciones de competencia.

vi) Incentivar la inversión en redes para la provisión de internet fijo y móvil con mayor calidad y más cobertura.

Aunque a primera vista es claro que estos lineamientos comparten una visión afín a los intereses de la industria de telecomunicaciones y el desarrollo de esta, el documento en el que se presentaban estos lineamientos contaba una versión distinta a los objetivos mencionados anteriormente. El anteproyecto mostraba lineamientos que otorgaban al Estado la facultad de remover contenidos, aplicaciones y servicios de

internet, también permitía el monitoreo del tráfico de internet a través de la inspección profunda de paquetes, permitía la priorización pagada de contenidos en beneficio de los socios comerciales de las empresas proveedoras de acceso a internet (interfiriendo directamente con el acceso a la información e incluso afectando las posibilidades de competencia justa para productores de contenidos y servicios independientes, en completa incongruencia con la neutralidad de la red) y, además, omitía los contrapesos necesarios para asegurar la protección de la neutralidad de la red.

En respuesta a estos lineamientos que buscan favorecer los intereses de la industria menoscabando nuestros derechos, a través de la campaña #SalvemosInternet[108] se logró convocar a más de 150 mil personas en todo el país para que se sumaran a la participación en la consulta pública manifestando las preocupaciones que prevalecen desde 2014; ya que tanto en los objetivos del anteproyecto como en el documento que describe la propuesta de lineamientos se hace patente que el interés principal para el desarrollo de esta propuesta no era la defensa de la neutralidad de la red ni de nuestros derechos digitales, sino la búsqueda por privilegiar los inte-

[108] Argüelles, A. (2020). "#SalvemosInternet para proteger nuestra democracia". *Derechos Digitales*. Disponible en https://www.mnemozine.xyz/blog/salvemosinternet-para-proteger-nuestra-democracia

reses de las empresas y consolidar mecanismos de vigilancia y control para el Estado. Precisamente los mismos motivos por los cuales tomamos las calles hace siete años.

El reconocimiento del acceso a internet parece una victoria absoluta en la consolidación de los derechos humanos que se amplifican a través de las tecnologías —lo que solemos llamar derechos digitales—, pero también en este logro vemos cómo los intereses de los actores preponderantes —en este caso las empresas y el gobierno— entran en tensión con la amplificación de nuestros derechos. Para evitar perder el poder consolidado, vemos cómo estos actores preponderantes terminan desarrollando medidas opacas muchas veces ilegibles para quienes no manejamos lenguajes altamente técnicos o jurídicos, e incluso surge el desarrollo a puerta cerrada de políticas pública que son aprobadas rápidamente —sin consulta pública previa— para menguar nuestros derechos. Estas tensiones políticas entre los intereses de la sociedad civil y los intereses de las empresas o industrias —que muchas veces también participan en intercambios comerciales con el gobierno, dando pie a lucrativos negocios y corruptelas que lamentablemente no son novedad en nuestro contexto—, devienen en prácticas desleales en las que se restringe, o activamente se ignora, la participación de la sociedad civil en la toma de decisiones que terminan dando forma al "conjunto de criterios que establecen los límites de las relaciones

en las que participamos” que a su vez constituye el sistema de “justicia” que nos gobierna.

Si bien el acceso a internet y el acceso a las tecnologías —particularmente las tecnologías de información y comunicación o TIC— podrían ser clave para la amplificación del ejercicio de derechos, es claro que si sus implementaciones no ponen al centro el bienestar y la dignidad de las personas, estas tecnologías —y las políticas públicas que promueven su uso— terminarán siendo instrumentalizadas para consolidar el poder o perpetuar abusos que podrían disfrazarse bajo un discurso de progreso e innovación, a costa de los derechos de todas las personas, pero poniendo en riesgo especial a quienes han sido históricamente vulneradas y excluidas de estos “avances” por cuestiones de género, lengua, nivel socioeconómico u origen étnico. Un ejemplo claro de esto se puede contemplar actualmente, ante la profundización de la brecha educativa a raíz de las medidas de confinamiento que surgieron por la pandemia de COVID-19 y que llevaron a que la Secretaría de Educación Pública (SEP) apostara a trasladar la oferta educativa presencial a programas digitales.

Estudiantes de la Normal Rural de Mactumactzá, en Chiapas, vivieron y denunciaron las consecuencias de esta medida que, en su dependencia tecnológica, les excluyó del sistema educativo[109]. El 18 de mayo de 2021 se congre-

[109] _____. (2021). “Mactumactzá: derecho a la

garon en Chiapa de Corzo para exigir que se respetara su derecho a la educación y les permitieran acceder a la posibilidad de presentar el examen de ingreso al ciclo escolar de forma presencial, con cuadernillos de papel y pluma, en lugar de la vía digital; ya que a pesar de que el acceso a internet es un derecho en México, de acuerdo a la *Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares* (ENDUTIH) 2020 únicamente el 50.4% de las áreas rurales están conectadas a internet. Tanto la Normal Rural de Mactumactzá como sus estudiantes conforman la otra mitad de la población que sin acceso a internet no pudo beneficiarse de los programas tecnosolucionistas que implementó la SEP —a los que, además de lo que implica el costo de conectividad, habría que sumar la posibilidad de conseguir algún dispositivo funcional y accesible para aprovechar el acceso a internet.

Ese mismo día, en respuesta a sus demandas expresadas a través de la legítima protesta, el Estado desplegó a la policía militarizada para llevar a cabo la detención arbitraria de 95 estudiantes de comunidades rurales e indígenas, 74 estudiantes fueron liberadas el 24 de mayo, denunciando abuso de autoridad, uso excesivo

---

educación, acceso a internet y violencia estatal". *Animal político*. Disponible en https://www.animalpolitico.com/blog-invitado/mactumactza-derecho-a-la-educacion-acceso-a-internet-y-violencia-estatal/

de la fuerza y violencia sexual. Sus familiares, así como familiares de los estudiantes que seguían detenidos, continuaron recibiendo violencia por parte del Estado —resultando en lesiones y quemaduras de gas también en menores de edad y adultos mayores— hasta los primeros días de junio, cuando fueron liberados.

A la fecha no hay información disponible sobre las medidas de reparación ni el acceso a la justicia que ofrecerá el Estado a través del gobierno local para resarcir los daños y asegurar los derechos de alrededor 480 jóvenes que asisten a la Normal Rural de Mactumactzá y que, de acuerdo con el antropólogo y activista Abel Barrera Hernández, en su mayoría pertenecen a los pueblos Tzeltal, Tzolzil, Tojolabal, Zoque, Chol y Mam. En respuesta a las demandas del 18 de mayo, se anunció que el examen se llevará a cabo de manera presencial el 9 de junio a través de dispositivos conectados a internet que el gobierno local pondrá a disposición, imponiendo el uso de estas tecnologías —frente a la demanda específica del uso de cuadernillos y plumas— bajo el pretexto de las medidas sanitarias.

Aunque podríamos asumir que la intención de la Secretaría de Educación Pública era noble y a grandes rasgos práctica, es simplemente inaceptable que una Secretaría del Estado promueva medidas tan sesgadas y simplistas, sin el mínimo reparo en cómo estas podrían amplificar o agravar las brechas de acceso a derechos de las personas que enfrentan condiciones distin-

tas a las que podríamos asumir que están presentes en las grandes áreas urbanas del país. Sin embargo, este fenómeno que pretende usar las tecnologías como soluciones únicas y definitivas no se ha limitado al sector educativo, sino que ha propagado otros sectores como el cultural, el laboral, el económico, la salud y el ámbito de la seguridad pública.

Pensar las tecnologías de esa forma tan arbitraria demuestra el desconocimiento que existe sobre ellas y nos condena a vivir en una sociedad a la que se le niega la participación informada —y el consentimiento— respecto de las tecnologías que están siendo usadas para dar forma al futuro que habitaremos. Las tecnologías no son soluciones, las tecnologías son herramientas que pueden ayudarnos a encontrar las soluciones multidisciplinarias y flexibles que ameritan los problemas complejos en los contextos diversos que vivimos; sin embargo, si las tecnologías se implementan de forma sesgada y totalitaria —sin espacio a discusión, diálogo e incluso sin periodos de prueba— probablemente existan otros intereses para los cuales las tecnologías se vuelven instrumentos indispensables, como se ha visto en la consolidación de capacidades de control y vigilancia que se han extendido en los últimos años a lo largo de América Latina.

Además, las tecnologías vienen envueltas en sus propias complejidades, no están libres de conflicto y definitivamente no son neutrales. Cabe cuestionarnos quiénes desarrollan los dis-

positivos y plataformas que usamos, quién está detrás de los acuerdos comerciales que establecen el uso de un servicio sobre otro o incluso cuáles son las opciones de accesibilidad que existen para que estas tecnologías no únicamente lleguen, sino que puedan ser aprovechadas por personas con discapacidad o que únicamente hablan lenguas indígenas. Volviendo al caso de Mactumactzá, necesitamos conocer las necesidades de infraestructura que requieren las tecnologías para operar, así como también entender los impactos que estos despliegues tienen para nuestros entornos, tanto en el consumo de recursos naturales como en el medio ambiente. Por poner un par de ejemplos, pensemos en el impacto ambiental que tienen las granjas de servidores o los desechos digitales.

Algo que se suma a la gravedad respecto a la implementación de medidas tecnosolucionistas, particularmente las que se despliegan bajo el discurso de la supuesta "seguridad", tiene que ver con las obstrucciones que estas representan para los mecanismos de transparencia y rendición de cuentas. Antes de ir hacia las tecnologías más recientes y sofisticadas, en el ejercicio de preservación de la memoria, me gustaría recordar el caso del sitio 1DMX. En diciembre de 2012, tras la toma de poder de Enrique Peña Nieto, las agresiones físicas y detenciones arbitrarias de periodistas y personas que participaron en distintas protestas alrededor del país fueron ampliamente documentadas

por esfuerzos independientes que buscaban generar contrapesos a los cercos mediáticos establecidos por los medios de comunicación, que muchas veces terminaban cediendo a las presiones gubernamentales para presentar información sesgada o simplemente negar la cobertura a hechos en los que las violencias por parte del Estado y las violaciones graves a los derechos humanos eran evidentes. Así el 1dmx.org se convirtió en un repositorio abierto de evidencias de los abusos que habían surgido y de los cuales el gobierno en turno negaba rotundamente su existencia.

A un año de la creación del sitio, este fue dado de baja a través de la colaboración entre el gobierno de México y el gobierno de Estados Unidos. Poco después de que se inició un juicio de amparo que obligaba a la Secretaría de Gobernación y a la Comisión Nacional de Seguridad a brindar información sobre su participación en la remoción del sitio, estas instancias se negaron a cooperar en la investigación. Cabe mencionar que el comisionado a cargo de la Comisión Nacional de Seguridad, en aquel entonces, era también el responsable de los operativos que reprimieron tanto la protesta como las coberturas del 1 de diciembre de 2012. Tiempo después, GoDaddy —la empresa que alojaba el sitio— dijo que la solicitud de remoción había surgido del Centro Especializado en Respuesta Tecnológica (CERT), una dependencia de la Policía Federal de la Comisión Nacional de Seguridad.

Aunque probablemente este sea uno de los primeros casos mediáticos sobre la censura en internet habilitada por el Estado mexicano, definitivamente no cesaron ahí los intentos por consolidar otros mecanismos que surtieran estos efectos. Sin embargo, ahora los mecanismos de censura en internet se han ido sofisticando junto a los discursos con los que pretenden ser legitimados. Recientemente hemos visto cómo la censura ha avanzado a través de los acuerdos comerciales internacionales que incorporan medidas en beneficio de las industrias de propiedad intelectual y entretenimiento globales (como el Digital Millenium Copyright Act o DMCA), mientras menoscaban nuestros derechos; como se manifestó en la campaña #NiCensuraNiCandados[110], frente a las reformas que se hicieron a la Ley Federal del Derecho de Autor y el Código Penal Federal derivadas del Capítulo de Propiedad Intelectual del Tratado entre México, Estados Unidos y Canadá (TMEC). Por otro lado, incluso las "normas comunitarias" de las plataformas de redes sociodigitales más populares son usadas para remover contenidos afines a las protestas sociales, así como contenidos sobre salud sexual y reproductiva que permiten revertir los efectos

[110] _____. (2020). "¿Pero qué necesidad? Los derechos humanos NO son moneda de cambio". *Derechos Digitales*. Disponible en https://www.mnemozine.xyz/blog/2021/5/13/pero-qu-necesidad-los-derechos-humanos-no-son-moneda-de-cambio

de las políticas ultraconservadoras que nos han privado de esta información por generaciones.

Estas medidas, tan llenas de intermediación, dificultan que se pueda dar un seguimiento eficaz y claro que permita rastrear el origen de la censura; habilitando el abuso de estos mecanismos por la impunidad que permiten para quienes solicitan la remoción de contenidos a través de ellos, aun cuando los contenidos removidos sean de interés público. Esta instrumentación de las tecnologías, en un país con índices tan altos de violencia contra periodistas, activistas y personas defensoras de derechos humanos como México, constituye una mordaza para la libertad de expresión y un obstáculo para el acceso a la información que obstruye también el acceso a la justicia cuando se busca encontrar a quienes resultan responsables de esta censura digital.

Algo similar ocurre con los mecanismos de vigilancia e intervención de telecomunicaciones en nuestro país. Desde 2010, como refleja el resumen de vigilancia digital publicado por Sursiendo en 2019, han existido diversos casos donde las tecnologías se han usado para espiar a periodistas, activistas y personas defensoras de derechos humanos a través de la vulneración de su privacidad. Probablemente los casos que generaron más eco fueron los relacionados al informe #GobiernoEspía, publicado por la Red en Defensa de los Derechos Digitales (R3D) en 2017, en el que se evidencia la adquisición y el uso ilegal de herramientas de vigilancia por parte de las

autoridades mexicanas. Aunque frente a este caso se presentaron diversas medidas nacionales e internacionales para denunciar y condenar públicamente estas intervenciones abusivas, en años recientes hemos sabido de otros sistemas de vigilancia que han sido adquiridos por el Estado mexicano haciendo caso absolutamente omiso de las demandas que se han presentado por el uso abusivo e ilegal de estas tecnologías en años anteriores. En diciembre de 2020, a partir de una investigación realizada por Citizen Lab, se hizo de conocimiento público que México era el principal comprador de sistemas desarrollados para explotar vulnerabilidades en teléfonos celulares con el fin de acceder a llamadas, mensajes de texto y datos de localización. En abril de 2021, se reveló que la Fiscalía General de la República incumple con los controles judiciales al continuar adquiriendo servicios de geolocalización masiva e indiscriminada que ha utilizado desde 2018 sin haber solicitado autorización judicial. Estas actividades, constatadas por la Auditoría Superior de la Federación, se hicieron de conocimiento público a partir de un reportaje de Zorayda Gallegos publicado por *El País*[111]. Hasta

[111] Gallegos, Z. (2021). "La Fiscalía de México ha contratado en los dos últimos años programas para el espionaje masivo de teléfonos móviles". *El País*. Disponible en https://elpais.com/mexico/2021-04-14/la-fiscalia-de-mexico-ha-contratado-en-los-dos-ultimos-anos-programas-para-el-espionaje-masivo-de-telefonos-moviles.html

ahora, todas estas actividades ilegales que constituyen abusos de poder por parte del Estado y que violan directamente el derecho a la privacidad permanecen impunes o atrapadas en largos procesos de investigación que no han logrado brindar acceso a la justicia para quienes fueron víctimas de estas intervenciones.

En febrero de 2021, Madeleine Wattenbarger publicó un reportaje con el título "Donde funcionan las cámaras de vigilancia, pero la justicia no"[112] que —en un caso similar a lo que ocurre con los sistemas de espionaje digital— señala cómo en México, particularmente en la Ciudad de México, contamos con uno de los sistemas de videovigilancia más sofisticados del mundo que, a pesar de toda su potencia, no sirve para prevenir los delitos ni para procurar el acceso a la justicia. Los despliegues de cámaras de videovigilancia en el espacio público no son recientes, sin embargo, también se han ido sofisticando a pesar de que su uso se ha estado prohibiendo en varias ciudades alrededor del mundo porque al ser altamente invasivas estas tecnologías producen efectos inhibitorios en las personas, comprometiendo su libertad de tránsito y su privacidad. En Coahuila, un estado fronterizo al norte de México, en 2019, se inició la instalación de

[112] Wattenbarger, M. (2021). "Donde funcionan las cámaras de vigilancia pero la justicia no". *rest of world.* Disponible en https://restofworld.org/2021/donde-funcionan-las-camaras-de-vigilancia-pero-la-justicia-no/

cámaras de videovigilancia en el espacio público, que además poseen tecnologías de reconocimiento facial: tecnologías de vigilancia biométrica. En noviembre de 2020, una investigación publicada por Quinto Elemento Lab evidenció que incluso los protocolos internos establecidos por la fiscalía local para agregar imágenes a la base de datos de identificación habían sido descartados para responder a una petición de búsqueda realizada por el FBI, a fin de continuar la persecución de dos estadounidenses que participaron en las protestas antirracistas tras el asesinato de George Floyd a manos de policías en Minneapolis. En México ni la persecución de activistas ni la siembra de evidencia para incriminarles son nuevas, tampoco lo es la colaboración con el gobierno estadounidense. Bajo la presunción de terrorismo, actualmente los sistemas de reconocimiento facial mexicanos participan en la persecución de este par de activistas.

Las tecnologías de videovigilancia masiva en el espacio público, así como las tecnologías de vigilancia biométrica, también han sido denunciadas a nivel internacional por los efectos negativos que tienen sobre nuestros derechos, pero también porque han generado altas tasas de falsos positivos que criminalizan a personas que pertenecen a grupos que han sido históricamente vulnerados por cuestiones étnicas. A esta discriminación que se amplifica en los sesgos de estas tecnologías, se suma también la discriminación que se ha denunciado por parte

de integrantes de la comunidad trans, quienes terminan recibiendo revictimización por parte de estos sistemas que les niegan el reconocimiento de su identidad de género (aun cuando esta sea reconocida en documentos oficiales). A pesar de todo esto, a la fecha, los sistemas de videovigilancia y la vigilancia biométrica en el espacio público se siguen promoviendo por parte de las instancias tanto gubernamentales como encargadas de la seguridad nacional. De nuevo, descartando por completo las preocupaciones que desde la sociedad civil se han presentado respecto a la violencia que su uso representa para los derechos humanos y la falta de contrapesos o salvaguardas que efectivamente permitan que las personas estemos seguras, aun frente al uso de abusivo de estas tecnologías altamente invasivas y completamente inútiles —como expone el reportaje de Madeleine— para el acceso a la justicia.

La intención de consolidar bases de datos que nutran las tecnologías de identificación biométrica en nuestro país no termina ahí. En diciembre de 2020, la Cámara de Diputados aprobó la Ley General de Población que pretende garantizar el derecho a la identidad a través de una cédula de identidad digital que será operada y emitida por la Secretaría de Gobernación y, aunque no sustituirá otros documentos de identificación, servirá para consolidar otra base de datos altamente sensibles que estará en manos del Estado, pues esta cédula pretende incorporar datos

biométricos. Cuando hablamos de datos biométricos nos referimos a los marcos faciales, registros de iris, huellas digitales o hasta voz, pero también a cualquier dato sobre nuestro cuerpo que pueda ser recabado con el fin de hacernos identificables.

Algunas de las preocupaciones respecto a esta cédula tienen que ver con la falsa justicia que ofrece, ya que si bien se anuncia como una medida para "garantizar el derecho a la identidad", el uso de las tecnologías, por más sofisticadas o innovadoras que sean, no refleja realmente un compromiso por resolver la deuda pendiente que tiene el Estado con las poblaciones indígenas en el reconocimiento de su identidad e incluso —tomando de ejemplo lo ocurrido en la Normal Rural de Mactumactzá— resulta obvio deducir que esta medida podría amplificar las brechas relacionadas a la falta de rutas de acceso a la justicia o, en este caso, la falta de acceso al reconocimiento de la identidad por parte del Estado. Esto podría generar aún más obstrucciones para el reconocimiento de los derechos de estas poblaciones; pero también genera mucha desconfianza respecto a la consolidación de bases de datos tan sensibles como los datos biométricos, pues el gobierno mexicano ha demostrado en varias ocasiones no tener la capacidad para proteger bases de datos personales que han sido vulneradas, como han sido los casos del INAI en 2020 o el IMSS en 2021. En enero de 2021, Rodrigo Riquelme publicó desde *El Econo-*

mista[113] un resumen de las 12 vulneraciones a bases de datos más graves que se reportaron en 2020 por instituciones públicas y privadas en el país, que vale la pena tener en mente.

En un esfuerzo similar por consolidar bases de datos biométricos, que incluso podrían ser usadas para nutrir los algoritmos de identificación que permiten la operación de las cámaras de vigilancia con reconocimiento facial en el espacio público, en diciembre de 2020 se aprobó una iniciativa para crear el Padrón Nacional de Usuarios de Telefonía Móvil (PANAUT) con la intención de que este registro pueda servir para reducir la extorsión telefónica en México. Esta iniciativa hace eco al RENAUT de 2011, registro que fue destruido un año después de su habilitación al demostrarse que no únicamente había resultado completamente inútil para reducir los índices de extorsión, sino que había permitido que se generaran casos de suplantación de identidad y desde su implementación la incidencia en extorsión había incrementado en más de 40% para el 2012. Si bien esta iniciativa nace, como muchas de las anteriores, como una respuesta para "mejorar la seguridad", en un contexto como el que enfrentamos ahora, ante una grave crisis económica tras la contingencia sanitaria por COVID-19,

[113] Riquelme, R. (2021). "2020, en 12 hackeos o incidentes de seguridad en México". *El Economista*. Disponible en https://www.eleconomista.com.mx/tecnologia/2020-en-12-hackeos-o-incidentes-de-seguridad-en-Mexico-20210102-0007.html

resulta completamente innecesario y desleal dirigir inversiones millonarias a este tipo de medidas que se ha demostrado que son inútiles.

La diferencia entre el PANAUT de 2020 y el RENAUT de 2011 es que el PANAUT busca sumar datos biométricos —aunque no ha quedado claro cuáles— a su registro. Algo que es muy importante mencionar aquí es que aunque esta medida se ofrece como una respuesta para mejorar la "seguridad", al no haber claridad sobre sus implicaciones tampoco existe la posibilidad de participar de manera informada, por lo que —de aprobarse esta medida— se nos negaría la posibilidad de otorgar o reservar el consentimiento sobre la captura de nuestros datos —también los biométricos— y además se contravendrían nuestros derechos ARCO (Acceso, Rectificación, Cancelación y Oposición). Lo anterior agrava el hecho de que en la participación coercitiva en este padrón también se supedita el derecho a la comunicación, ya que —en teoría— si no participamos en el PANAUT se nos restringiría la posibilidad de contratar una línea telefónica. Pensar que el crimen organizado no tiene formas para eludir estas medidas es completamente ingenuo e incluso necio frente a la evidencia que dejó la experiencia con el RENAUT, sin embargo, esto podría amplificar —nuevamente— las brechas que dificultan el acceso a las telecomunicaciones, obstruyendo tanto el ejercicio de derechos como el acceso a tecnologías que puedan servir como herramientas para avanzar en el acceso a la justicia.

Como fue el caso de las campañas #SalvemosInternet —o su antecesora #NoMásPoderAlPoder, en 2014— y #NiCensuraNiCandados, frente al PANAUT la sociedad civil se organizó en torno a la campaña #NoAlPadrón. Esta campaña además de generar información respecto a las implicaciones del padrón y generar conciencia en torno a los datos personas y la defensa de derechos digitales, también ofrecía rutas de participación política en las que, más allá de tomar las redes sociodigitales más populares para abrir espacios de diálogo sobre estos temas, se habilitó la posibilidad de generar demandas de amparo gratuitas a través de la plataforma https://noalpadron.mx. Este es un claro ejemplo de cómo las tecnologías pueden ser usadas incluso para fomentar el acceso a la justicia desde una perspectiva que incorpore la participación política diversa en la incidencia por la defensa de nuestros derechos.

Los ejemplos de las diferentes campañas, acciones e incluso las resistencias para generar incidencia en las políticas que afectan tanto positiva como negativamente el ejercicio de nuestros derechos a través de las tecnologías han sido fomentados a través del ejercicio de nuestros derechos digitales. Usamos las tecnologías como herramientas para compartir información, usamos las distintas plataformas para convocar y difundir recursos, nos comunicamos y generamos contrapesos a las narrativas hegemónicas para cuestionar los discursos que dicta el Estado.

Todas estas actividades que pasan por el acceso a la información, la libertad de expresión, el acceso a la cultura, el acceso a internet y, también, el derecho a la privacidad para resguardar nuestra identidad y proteger nuestros datos personales son formas en las que se manifiesta la construcción de la justicia que genera posibilidades de transformación frente a las brechas, desigualdades e imposiciones autoritarias que menoscaban nuestros derechos.

Para aprovechar las tecnologías como herramientas para el acceso a la justicia, volviendo a las preguntas con las que inicia este texto, es necesario conocer los alcances (y sesgos) que tienen y situarlas de forma que respondan a nuestras necesidades en un sentido amplio, que puedan abarcar la complejidad de nuestros contextos para evitar que las tecnologías se conviertan en barreras de discriminación. Para esto es importante romper con la engañosa noción de que las tecnologías son soluciones. Las soluciones fincadas en el compromiso social y el acceso a la justicia no pueden centrarse en la instrumentalización de herramientas, deben poner al centro la dignidad y el respeto a los derechos humanos para tejer, a partir de estas perspectivas, oportunidades creativas y locales, a fin de que se procuren entornos de innovación y desarrollo de tecnologías que respondan a nuestras necesidades específicas, sean accesibles y estén sujetas a mecanismos de transparencia —por parte de quienes las desarrollen y operen—, consenti-

miento y participación informada por parte de la población en general.

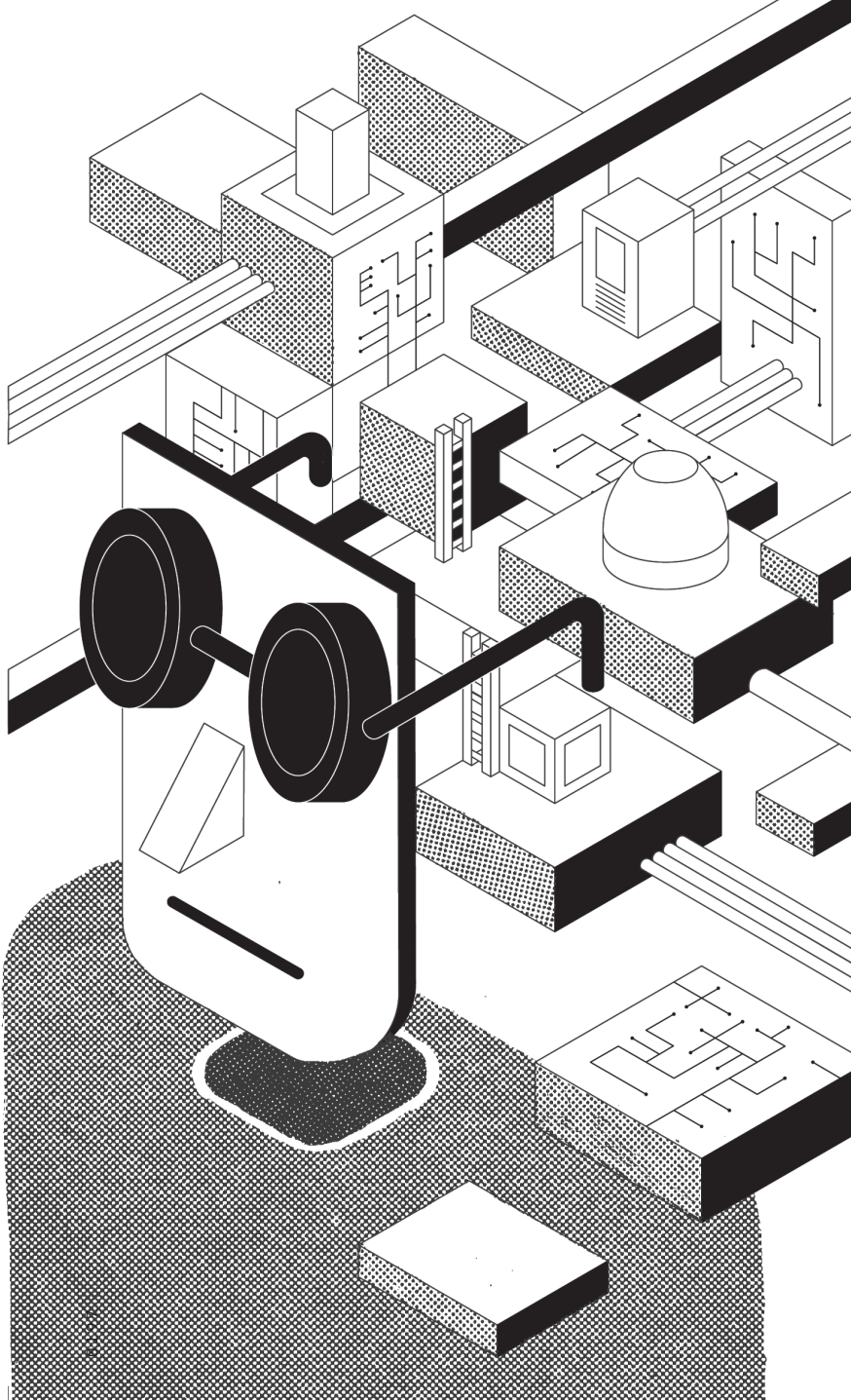
Parafraseando a Phi Requiem, consultor en seguridad digital para personas defensoras de derechos humanos: “Se usan tecnologías del futuro para resolver problemas del presente con legislaciones del pasado”. El costo que estos sesgos tienen para el ejercicio de nuestros derechos se ve reflejado en la autonomía que poco a poco se nos ha ido menguando ante la implementación de despliegues de tecnologías que suelen reforzar las desigualdades y abusos de poder, abonando a la construcción de posibilidades que habiliten un futuro donde el autoritarismo podría encontrar una fuente inagotable de control en el uso de las tecnologías que actualmente se están desplegando en nuestro país bajo una falsa promesa de seguridad.

Si no podemos participar en la construcción de nuestro futuro, también se nos está negando el acceso a la justicia. Por esto es sumamente importante fomentar la participación, fomentar las posibilidades de incidencia para que, de manera informada y organizada, podamos romper la opacidad que rodea estos temas y evitemos que se sigan instaurando medidas tecnosolucionistas que nos tomará años revertir.

El terreno de lo político siempre está en disputa. No podemos permitir que esas disputas se sigan librando entre los mismos actores, entre los mismos poderes que se han consolidado a partir de la invisibilización y el silencio al que nos

relegan, los espacios que excluyen a la sociedad civil, con nuestras perspectivas múltiples y características diversas. Es importante informarnos, organizarnos e incidir para recuperar las posibilidades de construir el acceso a la justicia que queremos gozar en el futuro y que se nos ha negado en el presente.

Resguardemos la memoria, no olvidemos que las tecnologías son herramientas, no soluciones. Aprendamos sobre las que existen y están disponibles, desarrollemos tecnologías nuevas y hagámoslas accesibles. Rompamos las lógicas del progreso acelerado, detengámonos a imaginar e inventar los cimientos sobre los cuales queremos construir el futuro. Construyamos rutas accesibles para una justicia que transforme nuestro presente y nos permita acceder a futuros de posibilidades y no nos aten a un futuro distópico en el que tengamos que resignarnos a la impotencia y el miedo que instaura el autoritarismo que silencia el consenso y la participación. Aún estamos a tiempo de actuar, hagámoslo juntæs.



>> NO HAY JUSTICIA SIN PARTICIPACIÓN DIVERSA.

>>>>>>>>>>>>>>>>>>>

>> NO HAY JUSTICIA SIN CONSENTIMIENTO INFORMADO.

>>>>>>>>>>>>>>>>>>>

>> NO HAY JUSTICIA SIN ACCESIBILIDAD.

>>>>>>>>>>>>>>>>>>>

>> NO HAY JUSTICIA SIN CONTRAPESOS A LOS PODERES PREPONDERANTES.

>> NO HAY JUSTICIA SIN TRANSPARENCIA.

>>>>>>>>>>>>>>>>>>>

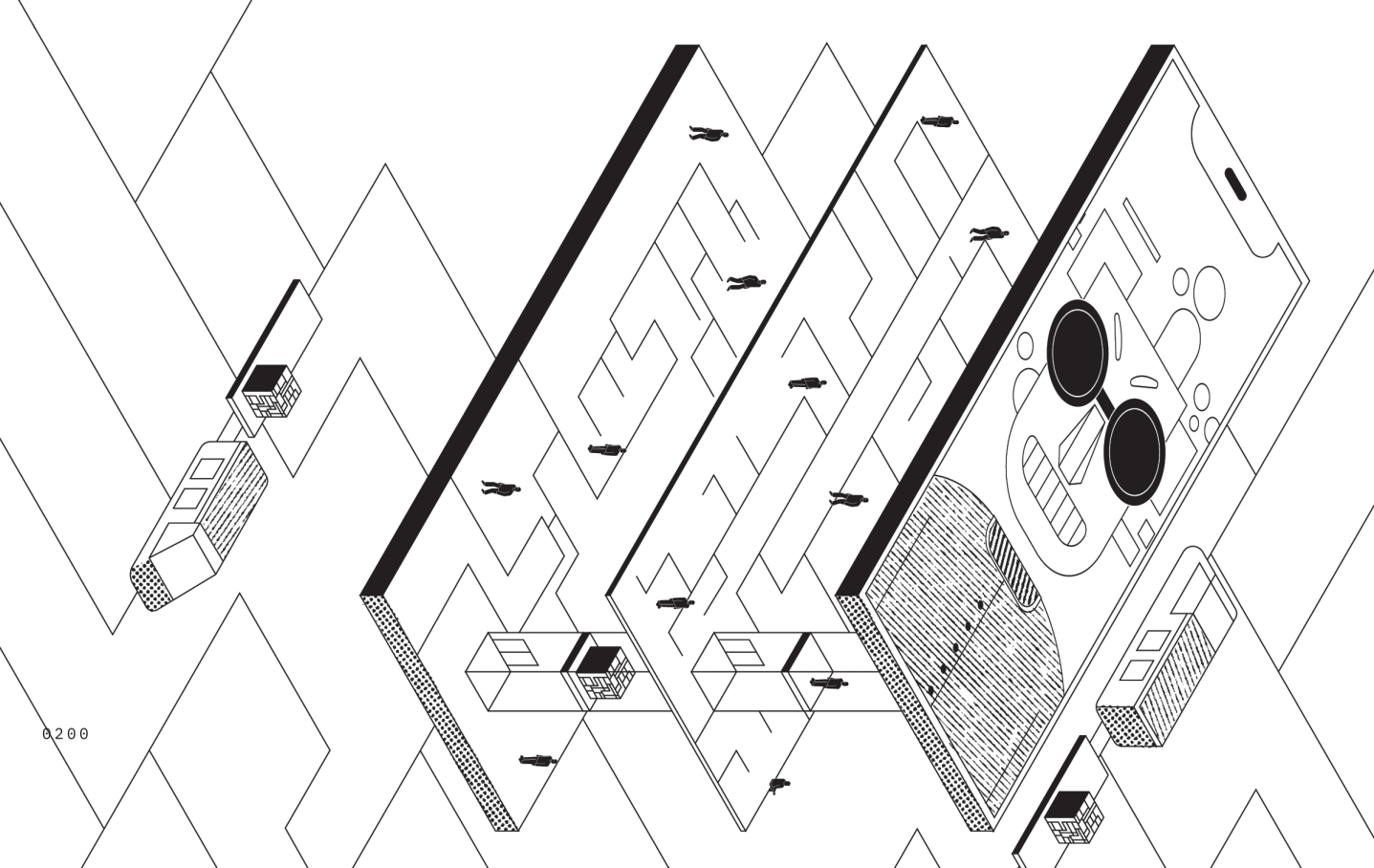
>> NO HAY JUSTICIA SIN RENDICIÓN DE CUENTAS.

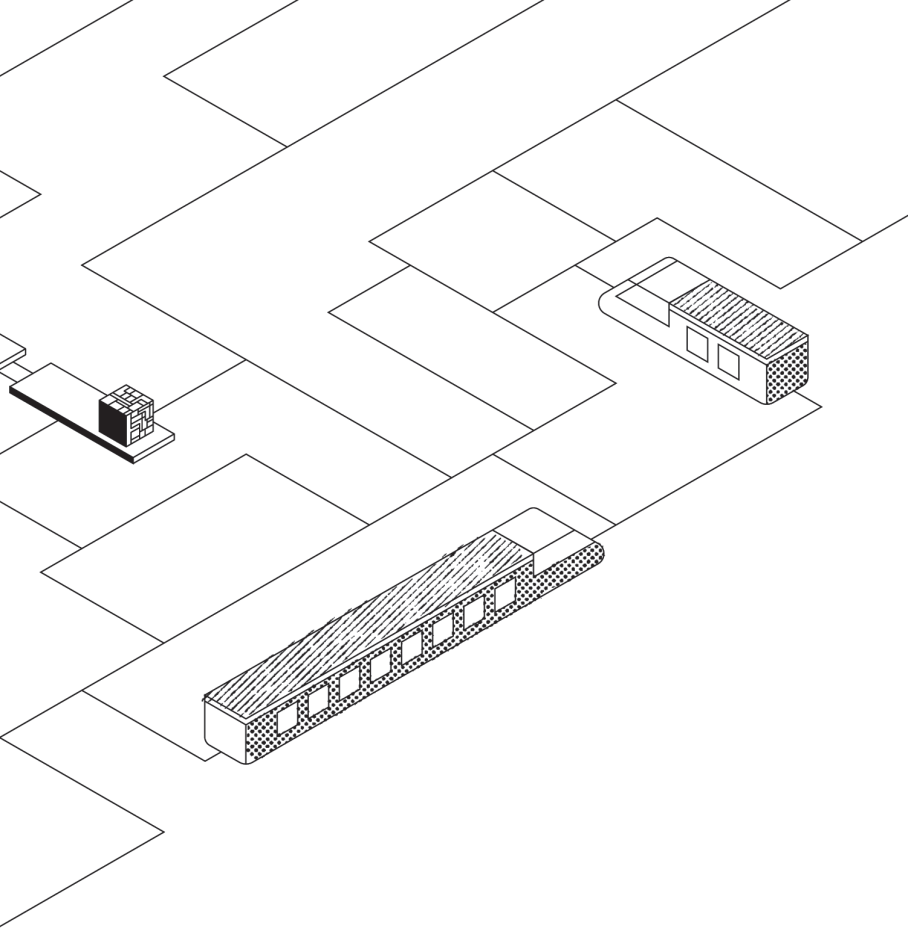
>>>>>>>>>>>>>>>>>>>

>> NO HAY JUSTICIA SIN MEMORIA.

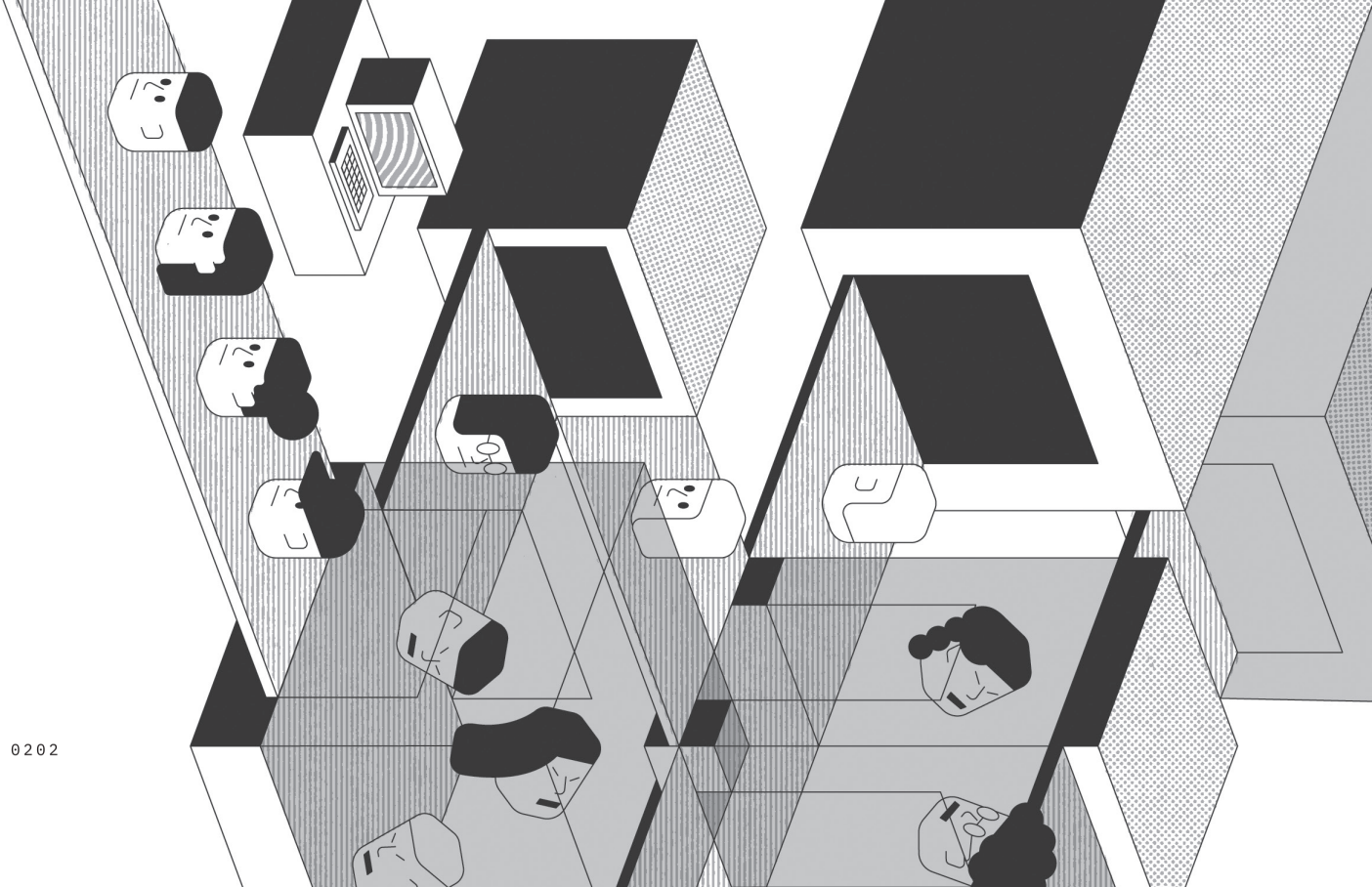
>>>>>>>>>>>>>>>>>>>

>> NO HAY JUSTICIA SIN TRANSFORMACIÓN.


0200



[Este texto es un homenaje]



Para más información sobre violencia digital en México, así como la versión digitalizada de este libro, eventos relacionados y recomendaciones actualizadas, visita nuestro sitio

- > **https://comun.al**

y ¡aprendamos juntæs!